A4 cncld.

selecting n plaintext blocks from said string in the same order as that used at the signing method, and combining said selected plaintext blocks and the random vector with a different corresponding element of said sequence of unpredictable elements to obtain a plurality of input blocks, in the same manner as that used at the signing method.

66. (Amended) The system as defined in claim 65, further comprising:

a third component for creating a secret random vector block of ℓ bits in length;

A5

wherein the first component performs the same randomization function as that used at the signing method over said plurality of plaintext blocks and the secret random vector block to create a plurality of input blocks each of ℓ bits in length;

wherein the first component performing said randomization function further comprises:

a component for deriving a random initial vector from said string presented for verification;

a component for generating a sequence of unpredictable elements each of ℓ-bit length from said random initial vector in the same manner as used at signing method; and

a component for selecting n plaintext blocks from said string in the same order as that used at the signing method, and combining said selected plaintext blocks and the random vector with a different corresponding element of said sequence of unpredictable elements to obtain a plurality of input blocks, in the same manner as that used at the signing method.

A6

72. (Amended) The program product of claim 71, wherein the third code for applying the pseudo-random function applies a pseudo-random function (41) that is a standard block cipher.

A7 cm.t

76. (Amended) The program product as defined in claim 75, further comprising:

seventh code for creating a secret random vector block of ℓ bits in length;

wherein the third code performs the same randomization function as that used at the signing method over said plurality of plaintext blocks and the secret random vector block to create a plurality of input blocks each of ℓ bits in length;

wherein the third code performing said randomization function further comprises:

code for deriving a random initial vector from said string presented for verification;

code for generating a sequence of unpredictable elements each of ℓ-bit length from said random initial vector in the same manner as used at signing method; and

A7 cncld.

code for selecting n plaintext blocks from said string in the same order as that used at the signing method, and combining said selected plaintext blocks and the random vector with a different corresponding element of said sequence of unpredictable elements to obtain a plurality of input blocks, in the same manner as that used at the signing method.

77. (Amended) The program product as defined in claim 75, wherein the third code for performing said randomization function further comprises:

code for using a secret, random initial vector shared between sender and receiver;

code for generating a sequence of unpredictable elements each of ℓ-bit length from said secret random initial vector in the same manner as used at signing method; and

code for selecting n plaintext blocks from said string in the same order as that used at the signing method, and combining said selected plaintext blocks with a different corresponding element of said sequence of unpredictable elements to obtain a plurality of input blocks, in the same manner as that used at the signing method.

Please add the following new claims 81-91:

81. (New) The method as defined in claim 1, wherein said partitioning said data into a plurality of data blocks further comprises data padding.

A8 cm't

82. (New) The method as defined in claim 7,

wherein said combining to create a plurality of input blocks comprises an operation that has an inverse, and

wherein the result of the combination of any two different unpredictable elements of the sequence of unpredictable elements by said inverse operation is unpredictable; and

wherein said unpredictable elements selected as said two unpredictable elements are any two different elements of the same sequence of unpredictable elements used for the signing of said plaintext string; and

wherein said unpredictable elements selected as said two unpredictable elements are any two different elements of a plurality of sequences of unpredictable elements used for the signing of a plurality of plaintext strings with the same secret key K.

83. (New) The method as defined in claim 7, wherein

if said combining to create a plurality of input blocks comprises an addition modulo 2^ℓ operation, the result of the combination of any two different unpredictable elements of the sequence of unpredictable elements by a subtraction modulo 2^ℓ operation is unpredictable;

else if said combining to create a plurality of input blocks comprises a bit-wise exclusive-or operation, the result of the combination of any two different unpredictable elements of the sequence of unpredictable elements by a bit-wise exclusive-or operation is unpredictable;

else if said combining to create a plurality of input blocks comprises a subtraction modulo 2^ℓ operation, the result of the combination of any two different unpredictable elements of the sequence of unpredictable elements by an addition modulo 2^ℓ operation is unpredictable; and

wherein said unpredictable elements selected as said two unpredictable elements are any two different elements of the same sequence of unpredictable elements used for the signing of said plaintext string; and

wherein said unpredictable elements selected as said two unpredictable elements are any two different elements of a plurality of sequences of unpredictable elements used for the signing of a plurality of plaintext strings with the same secret key K.

84. (New) The method as defined in claim 37,

wherein said combining to create a plurality of input blocks comprises an operation that has an inverse, and

wherein the result of the combination of any two different unpredictable elements of the sequence of unpredictable elements by said inverse operation is unpredictable; and

wherein said unpredictable elements selected as said two unpredictable elements are any two different elements of the same sequence of unpredictable elements used for the signing of said plaintext string; and

wherein said unpredictable elements selected as said two unpredictable elements are any two different elements of a plurality of sequences of unpredictable elements used for the signing of a plurality of plaintext strings with the same secret key K.

A8 cm.1

85. (New) The method as defined in claim 37, wherein

if said combining to create a plurality of input blocks comprises an addition modulo 2^ℓ operation, the result of the combination of any two different unpredictable elements of the sequence of unpredictable elements by a subtraction modulo 2^ℓ operation is unpredictable;

else if said combining to create a plurality of input blocks comprises a bit-wise exclusive-or operation, the result of the combination of any two different unpredictable elements of the sequence of unpredictable elements by a bit-wise exclusive-or operation is unpredictable;

else if said combining to create a plurality of input blocks comprises a subtraction modulo 2^ℓ operation, the result of the combination of any two different unpredictable elements of the sequence of unpredictable elements by an addition modulo 2^ℓ operation is unpredictable; and

wherein said unpredictable elements selected as said two unpredictable elements are any two different elements of the same sequence of unpredictable elements used for the signing of said plaintext string; and

wherein said unpredictable elements selected as said two unpredictable elements are any two different elements of a plurality of sequences of unpredictable

elements used for the signing of a plurality of plaintext strings with the same secret key K.

86. (New) The program product defined in claim 71, wherein the program code for causing the performance of the step of partitioning said data into a plurality of data blocks further comprises data padding.

87. (New) The program product defined in claim 77,

wherein the program code for causing the performance of the step of combining to create a plurality of input blocks comprises an operation that has an inverse, and

wherein the result of the combination of any two different unpredictable elements of the sequence of unpredictable elements by said inverse operation is unpredictable; and

A8 Cm.1

wherein said unpredictable elements selected as said two unpredictable elements are any two different elements of the same sequence of unpredictable elements used for the signing of said plaintext string; and

wherein said unpredictable elements selected as said two unpredictable elements are any two different elements of a plurality of sequences of unpredictable elements used for the signing of a plurality of plaintext strings with the same secret key K.

88. (New) The program product defined in claim 76, wherein

if the program code for causing the performance of the step of combining to create a plurality of input blocks comprises an addition modulo 2^ℓ operation, the result of the combination of any two different unpredictable elements of the sequence of unpredictable elements by a subtraction modulo 2^ℓ operation is unpredictable;

else if the program code for causing the performance of the step of combining to create a plurality of input blocks comprises a bit-wise exclusive-or operation, the result of the combination of any two different unpredictable elements of the sequence of unpredictable elements by a bit-wise exclusive-or operation is unpredictable;

else if the program code for causing the performance of the step of combining to create a plurality of input blocks comprises a subtraction modulo 2^ℓ operation, the result of the combination of any two different unpredictable elements of

the sequence of unpredictable elements by an addition modulo 2^{ℓ} operation is unpredictable; and

wherein said unpredictable elements selected as said two unpredictable elements are any two different elements of the same sequence of unpredictable elements used for the signing of said plaintext string; and

wherein said unpredictable elements selected as said two unpredictable elements are any two different elements of a plurality of sequences of unpredictable elements used for the signing of a plurality of plaintext strings with the same secret key K.

89. (New) The system defined in claim 61, wherein the partitioner component partitioning said data into a plurality of data blocks further comprises a component for data padding.

90. (New) The system defined in claim 66,

wherein the component for creating a plurality of input blocks comprises a component for an operation that has an inverse, and

wherein the result of the combination of any two different unpredictable elements of the sequence of unpredictable elements by said inverse operation is unpredictable; and

wherein said unpredictable elements selected as said two unpredictable elements are any two different elements of the same sequence of unpredictable elements used for the signing of said plaintext string; and

wherein said unpredictable elements selected as said two unpredictable elements are any two different elements of a plurality of sequences of unpredictable elements used for the signing of a plurality of plaintext strings with the same secret key K.

91. (New) The system defined in claim 66, wherein

if the component for creating a plurality of input blocks comprises a component for an addition modulo 2^{ℓ} operation, the result of the combination of any two different unpredictable elements of the sequence of unpredictable elements by a subtraction modulo 2^{ℓ} operation is unpredictable;

else if the component for creating a plurality of input blocks comprises a component for a bit-wise exclusive-or operation, the result of the combination of any

two different unpredictable elements of the sequence of unpredictable elements by a bit-wise exclusive-or operation is unpredictable;

A8 cncld.

else if the component for creating a plurality of input blocks comprises a component for a subtraction modulo 2^{ℓ} operation, the result of the combination of any two different unpredictable elements of the sequence of unpredictable elements by an addition modulo 2^{ℓ} operation is unpredictable; and

wherein said unpredictable elements selected as said two unpredictable elements are any two different elements of the same sequence of unpredictable elements used for the signing of said plaintext string; and